UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,400	11/03/2003	Anne Elizabeth Dudfield	12221-018001	6347

26161 7590 04/04/2008
FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
04/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/701,400	DUDFIELD ET AL.	
	Examiner	Art Unit	
	PRAMILA PARTHASARATHY	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 December 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/21/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to remarks filed on December 21, 2007. Claims 1 – 33 are pending.

Response to Arguments

2. Applicant's arguments with respect to non-statutory obviousness-type double patenting have been considered for the copending applications 10/701,154; 10/701,353; 10/701356 and 10/701,404 and Examiner withdraws the double patenting rejection as these copending applications are not yet ready for allowance. However, Examiner maintains double patenting rejection with respect to the now allowed copending application 10/701,376 (Notice of Allowability was mailed on 12/26/2007). Applicant argues that "copending application '376 (10/701,376) directed to finding anomalies by producing a moving average of a parameter associated with network packet flows", while the instant application uses connection pattern information not moving averages of parameters of network packet flows. Examiner disagrees and respectfully submits that

"receiving connection pairs from a connection table for a host that is attempting to gain access to another host in a networked computer system" and "determining if other anomalies in the connection patterns of each host exist to establish an event severity level indicating a likelihood that the host attempting to access another host is attempting an unauthorized access" regardless of the wording, still maps to "traversing a connection table that maps each host to a "host object" that stores information about all traffic to or from that host to determining connection patterns of a particular host in the network", and "identifying and correlating anomalies from the connection patterns with other found anomalies that exceed the threshold into at least one operationally relevant event indicating a detected event in the network", it is still determining anomalies and the language copending claims describes the structure of

determining anomalies that will be used to "detecting unauthorized access in the computer network".

Therefore, the main, and arguably only, difference in structure used make the determination about authorized access and/or unauthorized access, while the instant claims are broadly claiming the detection and determination of anomalies in the connection pattern, the copending claims are more specific as to the structure of "producing a moving average of a parameter associated with network packet flows" (please refer to 10/701,376 paragraph [0068 – 0071], it merely consist of a substitution of what is used to make that determination. Applicant's arguments are not persuasive.

3. Applicant's arguments with respect to prior art rejection have been fully considered but they are not persuasive for the following reasons: the applicant argues that the prior art Gupta et al. (Patent 7,234,168) does not disclose or suggest "retrieving connection pairs from a connection table for a host that is attempting to gain access to another host". This argument is not persuasive.

Gupta et al. teaches "an anomaly detector (62), which is used to identify network traffic anomalies indicative of an attack, and is implemented to create a characterization of the normal behavior of the system and detects anomaly for the observed packets based on the characteristics". Furthermore, Gupta teaches "The anomaly detector detects crafted packet attack or DDOS attacks based on the normal traffic profile of a target domain, which may be a single host/server, a sub-net, or an enterprise network" (See Gupta column 6 lines 3 – 42 and Column 7 lines 10 – 60).

Examiner further points out that "retrieving connection pairs from a connection table for a host that is attempting to gain access to another host" is not the heart of the invention. If the

applicant has the special method of retrieving connection pairs from a connection table then the examiner suggests amending the claims to explicitly recite such a retrieving technique.

A recitation directed to the manner in which a claimed apparatus is intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so perform (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987)). The prior art is replete with references disclosing "retrieving connection pairs from a connection table for a host that is attempting to gain access to another host". (See PTO 892).

Examiner also points out the instant invention is well depicted in Gupta Fig.2 and 3, Column 4 line 15 – Column 8 line 40 and Column 10 line 22 – Column 11 line 35, wherein Gupta teaches "determining other anomalies includes determining whether previous connection patterns of the hosts indicate that the hosts are in roles that are not normal for the hosts" see Gupta Column 6 lines 12 – 55 and connection patterns" (also, see above arguments supporting these additional limitations. Examiner maintains the rejection of Claims 1-33.

4. Examiner withdraws 35 USC 101 rejection.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., In re Berg, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); In re Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

5. Claims 1 – 33 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over amended claims 1 – 5, 7-9, 11-16 and 18-21 of copending application 10/701,376. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims correspond to the claims of the copending application, except in the instant claims the elements "retrieving connection pairs from a connection table for a host that is attempting to gain access to another host" referred in the copending claims as "traversing a connection table that maps each host to a host object that stores information about all traffic to or from that host to determine connection patterns of a particular host in the network". Copending claims recite, "identifying and correlating anomalies from the connection patterns with other found anomalies that exceed the threshold into at least one operationally relevant event indicating a detected event in the network" which encompasses the instant application claims "determining other anomalies includes using heuristics provide an indication to an operator that elevates severity of a possible unauthorized access event". Thus copending application claims anticipates the instant claims.

Claims of the instant application are anticipated by patent claims in that the patent claims contains all the limitations of the instant application. Claims of the instant application therefore is not patentably distinct from the earlier patent claims and as such are unpatentable for obvious-type double patenting *(In re Goodman (CAFC) 29 USPQ2d 2010 (12/3/1993).*

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Claims 1- 33 are rejected under 35 U.S.C. 102(e) as being anticipated by Gupta et al. (US Patent 7,234,168).

As per Claims 1, 12 and 23, Gupta teaches "retrieving connection pairs from a connection table for a host that is attempting to gain access to another host; determining whether that one host attempting to gain access has accessed the other host accessed previously; and if that one host has not accessed the other host previously, determining if other anomalies in the connection patterns of each host exist to establish an event severity level indicating a likelihood that the host attempting to access another host is attempting an unauthorized access" (Column 6 lines 3 – 42 and Column 7 lines 10 – 60).

As per Claims 2, 13 and 24, Gupta teaches "wherein determining other anomalies includes determining whether previous connection patterns of the hosts indicate that the hosts are in roles that are not normal for the hosts" (Column 7 lines 29 – 45).

As per Claims 3, 14 and 25, Gupta teaches "determining other anomalies includes determining whether the connection request uses the transport control protocol (TCP) (Column 7 lines 50 – 60)".

As per Claims 4, 15 and 26, Gupta teaches "determining other anomalies includes determining whether the connection requests use ports that are not well-known thus indicating a possible Trojan virus attack" (Column 9 lines 50 – 59).

As per Claims 5, 16 and 27, Gupta teaches "determining other anomalies includes using heuristics provide an indication to an operator that elevates severity of a possible unauthorized access event" (Column 23 lines 21 – 29).

As per Claims 6, 17 and 28, Gupta teaches "wherein determining other anomalies includes determining whether the connection requests use ports that have not been used previously" (Column 6 lines 3 – 11).

As per Claims 7, 18 and 29, Gupta teaches "wherein determining other anomalies includes determining if several short connections occur over a short time period by examining connection behavior between two hosts based on connection pattern data retrieved from the connection table" (Column 7 lines 19 – 28).

As per Claims 8, 19 and 30, Gupta teaches "determining whether conditions exist to decrease the severity assigned to an event" (Column 21 lines 21 – 39).

As per Claims 9, 20 and 31, Gupta teaches "determining whether conditions exist to decrease the severity assigned to an event, comprises: determining whether the hosts are in roles that commonly access each other's hosts" (Column 21 lines 21 – 39).

As per Claims 10, 21 and 32, Gupta teaches "determining whether conditions exist to decrease the severity assigned to an event, comprises: determining whether the host being connected to commonly receives connections from new hosts" (Column 21 lines 21 – 39).

As per Claims 11, 22 and 33, Gupta teaches "determining if other anomalies in the connection patterns of each host exist further comprises: determining whether conditions exist to decrease the severity assigned to an event; and if an event is still indicated, sending an event warning message with a determined level of severity to an operator" (Column 21 lines 21 – 39).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PRAMILA PARTHASARATHY whose telephone number is (571)272-3866. The examiner can normally be reached on 8:00a.m. to 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Pramila Parthasarathy/
Examiner, Art Unit 2136
March 30, 2008